International Journal of Engineering & Technology, 7 (3.24) (2018) 131-135

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Periocular Biometric Authentication Methods in Head Mounted Display Device

Sehee Kim[1], EuiChul Lee[*2]

[1]*Department of Computer Science, Sangmyung University20, Hongjimun 2-gil, Jongno-gu, Seoul, 03016, Republic of Korea*
[*2]*Department of Intelligent Engineering Informatics for Human, Sangmyung University20, Hongjimun 2-gil, Jongno-gu, Seoul, 03016, Republic of Korea*
**Corresponding author E-mail:eclee@smu.ac.kr*

Abstract

Background/Objectives: Recently, the use of Virtual Reality (VR) devices has increased and their content has also diversified. Therefore, content handling personal information is increasing, and a personal authentication method is needed. Currently, many VR devices are on the market; however, there is no method for personal authentication.
Methods/Statistical analysis: We acquire an eye image via an infrared camera attached inside a Head Mounted Display (HMD) for a VR experience, and propose a periocular biometric authentication method utilizing the eye image. The proposed method does not utilize high frequency components of the image, such as iris recognition; thus it has an advantage in that the recognition speed is fast, and the quality of the image is minimally affected. We used L1 distance, Local Binary Pattern (LBP), and Scale Invariant Feature Transform (SIFT) matching methods for eye image comparisons. In the matching process, a method for considering movement in horizontal and vertical directions was used to compensate for the position variation of the image.
Findings: Experimental results showed that the Equal Error Rate (EER) was the best at 6.83% for matching through the L1 distance. However, from a security viewpoint, it is confirmed that a False Rejection Rate (FRR) of approximately 10% is obtained when the False Acceptance Rate (FAR) is reduced to 0% through threshold adjustment. This result indicates that the proposed method can be fully utilized as a biometrics method for personal authentication.
Improvements/Applications: The proposed method is expected to be used as a biometric for personal authentication in existing HMD environments because it shows excellent performance with an EER of 6.83%, even when processing low frequency eye image components. Future research will investigate methods to improve in case of closed eye.

Keywords: *biometric authentication, periocular, head-mounted display device, VR device, L1 distance*

1. Introduction

Conventional methods for using personal information in software contents require additional input procedures. For example, the user must enter an ID and password, or store the authorized certificate on a storage medium and carry it. To improve this problem, authentication methods using biometrics are often used. Biometric authentication is convenient because it uses information from the user's body, thus avoiding the need for memorization or a separate input procedure[1]. Therefore, the technology is considered useful for non-face-to-face financial transactions, such as internet banking, smart banking, etc. [2].However, although user information obtained through biometric authentication is body-specific and an additional input procedure is not necessary, additional user cooperation is required[3].For example, it is necessary to match the iris to the camera for iris recognition and to attach the fingerprint to fingerprint identification equipment[4]. In this method, which is an advantage of convenience, this additional action may cause inconvenience.

As the use of virtual environment equipment increases, content becomes more diversified. Accordingly, a personal authentication method suitable for the VR environment is needed to protect personal information created from personalized contents. However, there are few personal authentication methods implemented in existing VR devices. For example, the user must manually input their ID and password. In the future, personal content will become more diverse, and personal data manipulation techniques must be developed[5]. In addition, VR devices have recently been equipped with an eye-tracking camera[6]. Accordingly, the eye image can be easily acquired through the camera in the device, and if the acquired image is used for authentication based on specific eye components, user authentication can be performed without additional input procedures or actions[7].

Among existing biometric authentication methods, there is an iris recognition system for authenticating the user based on eye images. Because the iris tissue of an individual must be identified in detail, image resolution must be high for this method [8] and, correspondingly, an expensive high-resolution camera is required [8,9]. In addition, the iris recognition method requires a large amount of computation because it extracts iris codes or uses complex expressions[10,11]. That is, the time complexity value is very large, and the operational speed is slow. However, the method proposed in this study provides personal authentication for images input with a low resolution camera (eye tracking camera); also, time complexity is reduced owing to a simple comparison operation. In terms of error rate, Biometric methods based on the entire eye image except the conventional iris recognition did not overcome the error rate of 10%[12]. In contrast, our proposed

method shows about 6% error rate, which is significantly improved compared to conventional biometric methods based on eye images.

For these reasons, the method proposed in this paper is suitable for use because VR content usage is increased and a Natural User Interface(NUI) is preferred[13].The proposed method is a non-intrusive one that allows the user wearing the HMD to operate without any conscious and unawareness. In addition, computation is fast, and the error rate is low. In this way, we can easily handle personal privacy information data in the VR environment, and our research is appropriate as a method for authentication.

2. Materials and Methods

The system flow chart of the proposed method is shown in Figure 1.The sentences appearing later in this paper will be described with reference to the labels ((a) - (i)) of this figure.

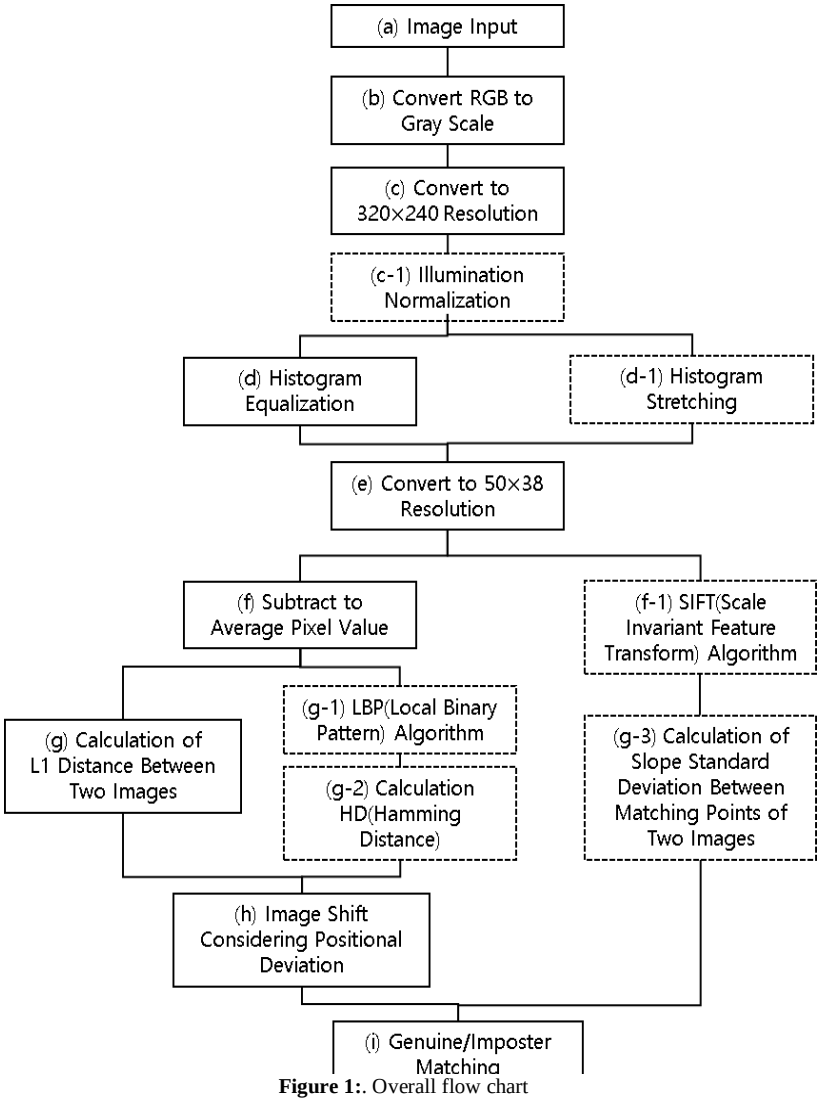
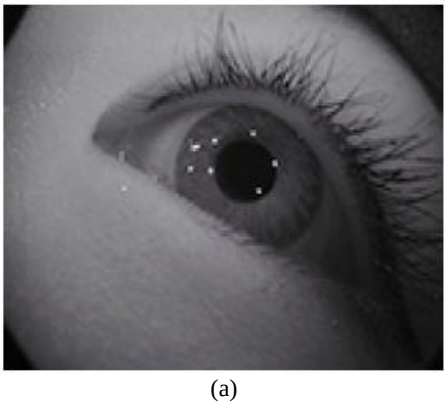
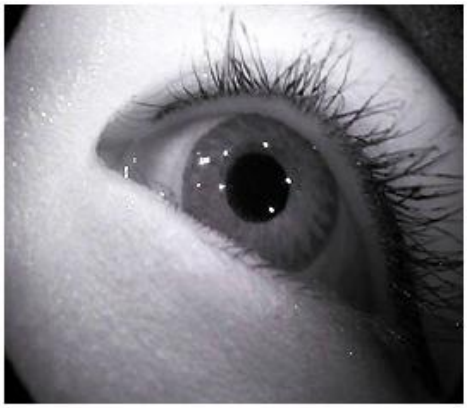


Figure 1:. Overall flow chart

(a) Input the images around the eyes from a camera attached to a wearable display device for virtual or augmented reality. To perform the biometric authentication method, in the image preprocessing process, (b) the image in the RGB domain is first converted into the gray scale, and (c) converted to a 320 × 240 image resolution. Illumination normalization was performed to make the transformed image more uniform[14].Illumination normalization is expected to improve the illumination difference in periocular images. However, because the difference in the degree of shading according to the user's eye curvature and contour is also a characteristic factor, the performance of non-normalized illumination is better. Therefore, (d) histogram equalization was performed without illumination normalization[14]. Figures 2 and 3 provide a comparison of the effect of the presence/absence of illumination normalization on Subject 1 before histogram equalization is performed on the two images. In the following figures, we can compare histogram equalized images with illumination normalization and histogram equalized images without illumination normalization.



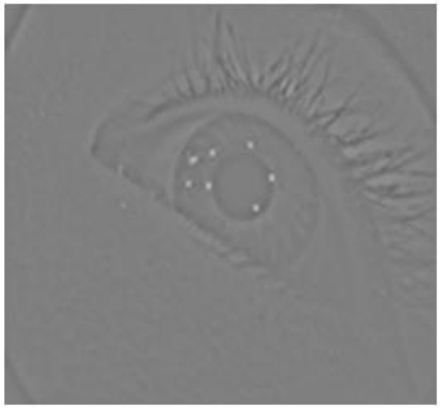
(a)



(b)

Figure 2:(a) Original input image of Subject 1, and (b) Image of histogram equalization without illumination normalization from (a)

(a)



(b)

(c)

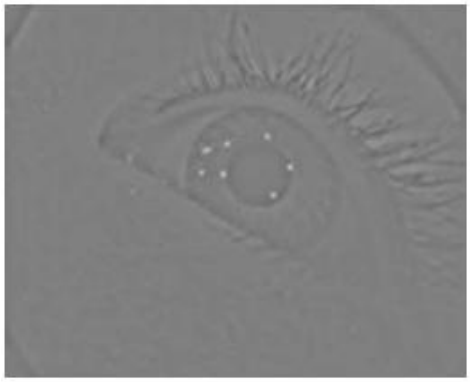
Figure 3:(a) Original input image of Subject 1, (b) Image of illumination normalization from (a),and (c) Image of histogram equalization from (b)

In other words, as shown in Figures 2 and 3, when the histogram equalization process is performed without illumination normalization in analyzing the eye image, the degree of the difference in the characteristics of the individual, the degree of bending of the eyes, and the skin is confirmed clearly. In addition, (d-1) histogram stretching was performed as a pre-test for image preprocessing; however, the best performance was achieved using only equalization[15].

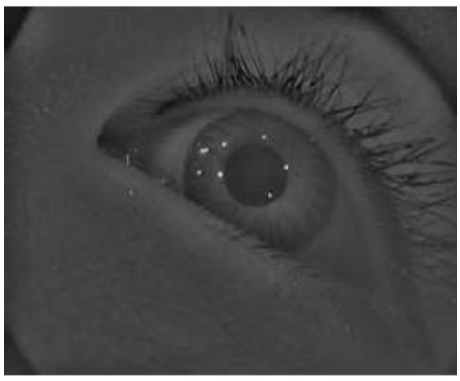
The reason for this result is that the histogram equalized image clearly shows the boundaries between the features of the subject, such as the eyes and the skin in the image; whereas, when histogram stretching is performed, the degree of shading of the image almost disappeared, such that it appears there is no difference between two images, even though it is the imposter matching case. As shown in Figure 4, it can be confirmed that the brightness of the image is darkened and the boundaries of each element, such as eyes, iris, and skin, are blurred over the eye image of Subject 1 as a whole.

In other words, histogram equalization is performed without illumination normalization to equalize the lightness and darkness of the image, and (e) the resolution is reduced to 50 × 38. By reducing the resolution of the image after equalizing to 50×38, high-frequency components, such as eye and eyebrow positions, are discarded because they are caused by slight positional changes that vary each time the equipment is worn. and the entire shape-based components of the eye remain; hence, they are not affected by the components that generate errors in authentication. To uniformize the illumination component in the transformed image, (f) the average brightness value of the image is subtracted from all the pixels of the image, such that the illumination deviation of the image is minimized.

(a)



(b)



(c)

Figure 4: (a) Original input image of Subject 1, (b) Image of illumination normalization from (a),and (c) Image of histogram stretching from (b)

When the preprocessing process is finished, the difference in the brightness of each pixel in the two images to be compared should be calculated. When each image is overlapped, the difference in the brightness value between pixels corresponding to the same position is obtained, and this value is added to obtain a total average value; (g) obtain the value for L1 distance calculation using Eq. 1:

$$L_1 = \frac{1}{MN}\sum_{i=0}^{N}\sum_{j=0}^{M}\left|P(x_i, y_j) - Q(x_i, y_j)\right| \quad (1)$$

At this point, the resolution of the image is $N \times M$ (50 × 38), which is the decimated resolution from the original image.

In this case, because the positional deviation may exist vertically and horizontally while the user is wearing equipment for two images, (h) image shifting processing which compensates for the variance of the image is necessary. As shown in Figure 5, two images are moved up and down by ± *h* pixels and left and right by ± *w* pixels, and authentication is performed at a point where the positional deviation of the two images becomes minimum. At this time, in the $N \times M$ image, *h* is set to approximately16% of *N* and *w* is set to approximately5% of M. The *h* deviation is set to be larger than the *w* deviation, because the vertical deviation is larger than the left-right deviation when the user wears the VR device on the head. In Figure 5, the enrolled image is an image in the database storing the user's pre-registered eye image, and the input image is the user's eye image when the user is wearing the wearable display device for virtual or augmented reality.

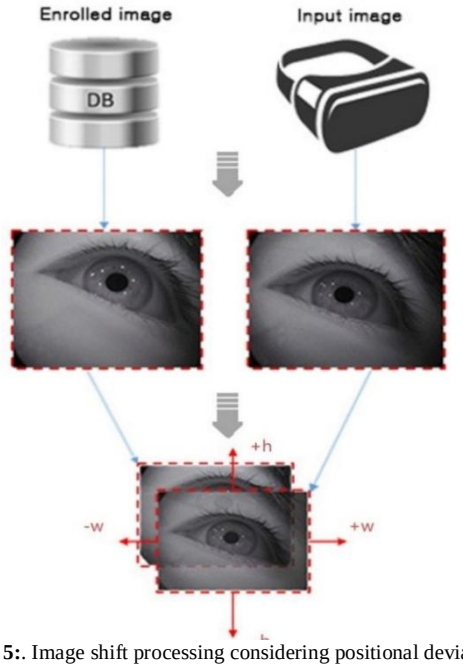


Figure 5:. Image shift processing considering positional deviation

3. Results and Discussion

In this paper, a total of 20 experiments were performed with the user wearing a display device for virtual or augmented reality; the test was repeated 10 times for each experiment, and a total of 200 experimental data were acquired by capturing images from 10 eyes. Through the method proposed in this paper, "genuine matching," which compares the eye images of the same person, and "imposter matching," which compares the eye images of others, were performed to obtain an EER of approximately6.83% and FAR of approximately 5.0%. In addition, we conducted a pre-test using the (g-1) LBP algorithm which verifies the identity of the two images considering their variants.(g-1) Using the LBP algorithm (g-2) to calculate the HD (Hamming distance), the minimum Hamming distance among the calculated Hamming distances is set as the threshold. When this method was used for self-certification, approximately12.5% of the EER and 0% of the FAR were derived. In addition, the (f-1) SIFT algorithm, another invariant method which does not take into account image variants, has been evaluated as a pre-test before proceeding with this study. SIFT matching of the two images to be compared comprises (g-3) calculating the slope standard deviation between the matching points of the two images, and setting the minimum value as the threshold value. In this method, because the positional deviation of two images is not considered, when there is an eye position deviation in the image, the slope standard deviation is calculated to be a large value even though it is the same person; hence, the error rate is also very large, approximately38.9% for EER and 15.3% for FAR.

Table 1 summarizes the EER and FAR derived from the three different methods mentioned in this paper, (g) L1 Distance, (g-1) LBP algorithm, and (f-1) SIFT algorithm.

Table 1: Equal Error Rate (EER) and False Acceptance Rate (FAR) percentages for the three methods

	L1 Distance	LBP Algorithm	SIFT Algorithm
EER	6.83	12.5	36.5
FAR	5.0	0	28

The distribution of L1 distance, Hamming distance, and slope standard deviation, which were calculated by three different methods, were statistically analyzed. As a result, as shown in Figure 6, the threshold value that best distinguishes a true identity from an imposter identity was calculated, and the identity authentication was performed based on the threshold. In addition, as shown in Figure 7, Receiver Operating Characteristic (ROC) curve, the method using the L1 metric, shows the best performance. Based on the results, we determined the L1 distance as the metric of authentication.

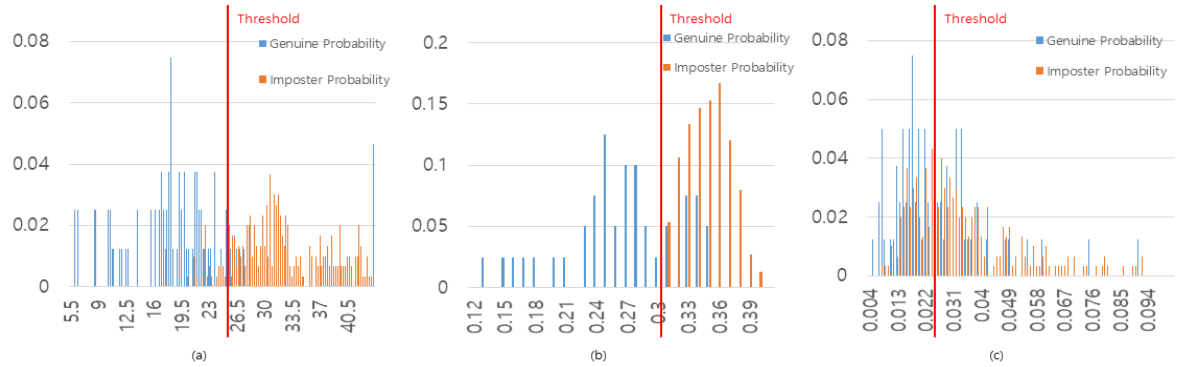


Figure 6:. Threshold calculated using (a) L1 distance, (b) LBP algorithm, and (c) SIFT algorithm (x-axis: Threshold, y-axis: probability)

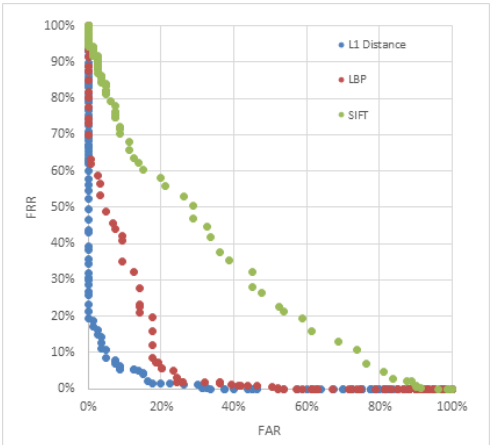


Figure 7:. ROC curve graph for three methods

4. Conclusion

In this paper, we propose a biometric authentication system that uses L1 distance as a metric for eye image based biometric authentication and utilizes an HMD that does not require additional user actions or equipment. Experimental results showed approximately 6.83% EER and 0.5% FAR. When dealing with data that contains personal privacy information, it is critical to reduce occurrences of false acceptance. In this study, a 0.5% FAR is suitable for managing security-sensitive data.

The biometric authentication system proposed in this paper, which is based on eye images obtained with a camera mounted on a wearable display device, exhibits excellent performance, a low time complexity, and a low resolution camera in comparison with a conventional iris image based authentication method. Hence, it is considered that this system can be usefully applied for the implementation of personal authentication processing in VR equipment.

Acknowledgment

This research was supported by a 2018 Research Grant from Sangmyung University.

References

[1] Oh S, Kang D. A Study on the RFID Biometrics System Based on Hippocampal Learning Algorithm Using NMF and LDA Mixture Feature Extraction. Journal of the Institute of Electronics Engineers of Korea SP 2006;43(4):46-54.

[2] K Gai, M Qiu, X Sun, H Zhao. Security and privacy issues: A survey on FinTech. International Conference on Smart Computing and Communication: Springer; 2016:236-247.

[3] Lim N, Ko D, Suh KH, Lee EC. Thumb Biometric Using Scale Invariant Feature Transform. Advanced Multimedia and Ubiquitous Engineering: Springer; 2017:85-90.

[4] Moon D, Gil Y, Ahn D, Pan S, Chung Y, Chung K. Implementation of A Security Token System using Fingerprint Verification. Journal of the Korea Institute of Information Security and Cryptology 2003;13(4):63-70.

[5] Kim J, Kwon Y. Therapeutic Virtual Reality Program in Chronic Stroke Patients Recovery of Upper Extremity and Neuronal Reorganization. Journal of Special Education & Rehabilitation Scienc 2005;44(1)87-106.

[6] Lee EC, Park KR. A robust eye gaze tracking method based on a virtual eyeball model. Mach Vision Appl 2009;20(5):319-337.

[7] Park KR, Kim J. A real-time focusing algorithm for iris recognition camera. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews) 2005;35(3):441-444.

[8] Joo S, Kang T, Yang W. A Implementation of Iris recognition system using scale-space filtering. The Journal of The Institute of Internet, Broadcasting and Communication 2009;9(5):175-181.

[9] Park K, Park S, Cho D. A Study on Eye Detection by Using Adaboost for Iris Recognition in Mobile Environments. Journal of the Institute of Electronics Engineers of Korea CI 2008;45(4):1-11.

[10] Matey JR, Naroditsky O, Hanna K, Kolczynski R, LoIacono DJ, Mangru S, et al. Iris on the move: Acquisition of images for iris recognition in less constrained environments. Proc IEEE 2006;94(11):1936-1947.

[11] Joo SH, Yang WS. A Study on the Size of 2D Iris Codes for Personal Identification. International Journal of Internet, Broadcasting and Communication 2011;11(2):113-118

[12] Cho SR, Nam GP, Shin KY, Nguyen DT, Pham TD, Lee EC, Park KR. Periocular-based Biometrics Robust to Eye Rotation Based on Polar Coordinates. Multimedia Tools and Applications 2017;76(9):11177-11197.

[13] Monro DM, Rakshit S, Zhang D. DCT-based iris recognition. IEEE Trans Pattern Anal Mach Intell 2007;29(4):586-595.

[14] Xie X, Lam K. An efficient illumination normalization method for face recognition. Pattern Recog Lett 2006;27(6):609-617.

[15] Pizer SM, Amburn EP, Austin JD, Cromartie R, Geselowitz A, Greer T, et al. Adaptive histogram equalization and its variations. Computer vision, graphics, and image processing 1987;39(3):355-368.